Bidirectional quantum secret sharing and secret splitting with polarized single photons

Fu-Guo Deng,[1,2,3,4*] Hong-Yu Zhou,[1,2,3] and Gui Lu Long[4,5†]

[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education,*
Beijing Normal University, Beijing 100875, China

[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering,*
Beijing Normal University, Beijing 100875, China

[3] *Beijing Radiation Center, Beijing 100875, China*

[4] *Key Laboratory For Quantum Information and Measurements of Ministry of Education,*
and Department of Physics, Tsinghua University, Beijing 100084, China

[5] *Key Laboratory for Atomic and Molecular Nanosciences, Tsinghua University, Beijing 100084, China*

(Dated: February 1, 2008)

In this Letter, we present quantum secret sharing and secret splitting protocols with single photons running forth and back between the participating parties. The protocol has a high intrinsic efficiency, namely all photons except those chosen for eavesdropping check could be used for sharing secret. The participants need not to announce the measuring bases at most of the time and this reduces the classical information exchanged largely.

PACS numbers: 03.67.Hk, 03.67.Dd, 89.70.+c

The security of the secret message transmitted has become one of the most important issues for modern economic and security activities. The goal of cryptography is to make secret message only readable for the two authorized parties, the sender, Alice and the receiver, Bob, and unintelligible for any unauthorized man, say an eavesdropper Eve. To date, the only proven secure crypto-system in the classical information theory is the one-time-pad scheme [1] in which the key is required to be as long as the message and is used just one time. The security of the message transmitted in this scheme depends entirely on the randomness of the private key. Alice and Bob have to distribute a lot of key before they start the secure communication. Quantum key distribution (QKD) has provided a secure way for transmitting private keys and it has progressed quickly [2] since an original QKD protocol was proposed by Bennett and Brassard, the BB84 scheme [3]. The nocloning theorem of quantum state [4] plays an important role in its security.

Another applications of quantum mechanics within the field of information is quantum secret sharing (QSS) which is a quantum counterpart of classical secret sharing [5]. One of the main goals of QSS is to distribute private keys among the three, or more generally, multi- parties securely. With the key, the sender, Alice can divide the message into N shares such that the other parties can read out the message only when they cooperate, and any set of less than N shares can get no information about the message. An original QSS scheme, the HBB99 scheme [6] was proposed by Hillery, Bužek and Berthiaume in 1999 using three-particle entangled Greenberger-Horne-Zeilinger (GHZ) states. In this scheme, the three parties, Alice, Bob and Charlie choose randomly two MBs, σ_x and σ_y to measure the particles in their hands independently. When they all choose σ_x or one chooses σ_x and the others choose σ_y, their results are correlated and will be kept for generating key, otherwise they discard the results. Its intrinsic efficiency, the ratio of number of theoretical valid transmitted qubits to the number of transmitted qubits is about 50% as half of the instances will be abandoned. Karlsson, Koashi and Imoto (KKI) put forward a QSS scheme [7] with two-photon polarization-entangled states, and its intrinsic efficiency is also 50%. Now, there are many theoretic and experimental studies on QSS, for instance in Refs. [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20].

Most existing QSS protocols use entangled states and the participants choose randomly one of two sets of measuring bases(MBs), for examples the protocols proposed in Refs. [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. The intrinsic efficiency of these protocols is usually 50%. Some techniques from QKD for improving the intrinsic efficiency [17, 21, 22] can be used for improving their efficiency in some QSS protocols. For example, the favored-measuring-basis technique [21] and the measuring-basis-encrypted technique [22] are extended to the multiparty QSS schemes in Ref. [16]. In the measuring-basis-encrypted QSS scheme, a three-party control key is generated first among the three parties, and they are used *repeatedly* to control the use of the alternative MBs. With a quantum storage [23, 24, 25], delayed measurement is possible and the efficiency of QSS can also be improved [17].

Entanglement is not necessary in quantum secret sharing. In Ref. [19], Guo and Guo proposed a QSS protocol without entanglement based on a modified BB84 QKD protocol and the efficiency is improved to approach 100%, with the use of quantum data storage. Single photons are ideal source for quantum communication. However at present, faint laser pulses are used to as approximate single photon sources. Recently we proposed a QKD pro-

[*] fgdeng@bnu.edu.cn

[†] gllong@tsinghua.edu.cn

tocol by using faint laser pulses travelling back and forth between the two parties [26].

In this Letter, we present a QSS protocol without entanglement by combining the idea for QSS with QKD [19] and the QKD protocol with faint laser pulses, the BID-QKD protocol in Ref. [26]. In the BID-QKD protocol, photon polarization states are used to encode information. First Bob prepares photons in one of the four possible states $|\pm z\rangle$, $\pm x\rangle$ randomly and then sends them to Alice. Alice performs some unitary operation to encode the information and then returns the photons to Bob. Bob reads out Alice's operation by making measurement. It was shown that the protocol is still secure if the number of photons in a pulse does not exceed two. Its intrinsic efficiency is improved to be 100%, and it does not require the use of a quantum data storage. Moreover, the classical information exchanged is reduced since the parties of communication need not to announce the information about the measuring basis (MB) in most instances. It is feasible with present-day technique. We also apply the idea to quantum secret splitting.

It is noted that any QKD protocol can be used for secret sharing if Alice can distribute a private key with each of the other parties. Let us use three parties, Alice, Bob and Charlie in secret sharing as an example, the naive-QKD QSS protocol. Alice creates the private key K_B with Bob, and K_C with Charlie. However one of the two parties Bob and Charlie maybe dishonest and the key they use to encrypt are denoted by K'_B and K'_C respectively. Alice needs to determine whether the key $K'_A = K'_B \oplus K'_C$ obtained by combining Bob's key and Charlie's key is the same as her key $K_A = K_B \oplus K_C$, where $\oplus$ means summing modulo 2. The process can be achieved by choosing random a sufficiently large subset of bits in the key K'_A to compare the results with those in the key K_A. If the error rate is zero, Alice confirms that there is no dishonest one among Bob and Charlie, and she sends the ciphertext to them after encrypting it with the key K_A; otherwise she has to abort the secret message communication. In this way, secret sharing can be accomplished with private keys and the main goal of QSS is to distribute a key among the parties efficiently.

QSS is more efficient for implementing the task of multi-party secret sharing than the above naive protocol based on QKD. QSS is also secure as the legitimate parties can determine eavesdropping. QSS also reduces the resource requirement [6, 7, 19]. A figure of merit is the total efficiency η defined as [27, 28].

$$\eta = \frac{b_s}{q_t + b_t}, \tag{1}$$

where b_s is the number of secret bits in the key, q_t is the number of qubit used, and b_t is the number of classical bits exchanged between the parties. For example, the total efficiency of BB84 [3] is $\eta = 25\%$ as half of the instances will be discarded and at least one bit of classical information exchanged for each qubit, i.e., $b_s = 0.5$, $q_t = 1$, $b_t = 1$. In the naive-QKD QSS protocol, Alice creates the keys K_B and K_C with Bob and Charlie respectively, and the total efficiency for a multi-party key is $\eta = \eta_{_B} \cdot \eta_{_C} = 12.5\%$. The HBB99 QSS protocol [6] needs one and half bits of classical information for each qubit and half qubit is useful. Its total efficiency is $\eta_{_{HBB99}} = \frac{0.5}{1+1.5} = 20\%$. So is the KKI QSS protocol [7].

In the following text, we present a QSS protocol using two bi-directional QKD protocols proposed in Ref. [26] with single photons. This protocol spares the use of quantum data storage. We will present the idea with a three-party case first, and the generalization to N parties is also presented.

For creating the key K_A, Alice prepares a two-photon product state $|\psi\rangle_A = |\phi\rangle_B \otimes |\phi\rangle_C$, and $|\phi\rangle_B$ and $|\phi\rangle_C$ are produced with two conjugate bases randomly: the rectilinear basis σ_z (i.e., $|+z\rangle = |0\rangle$, $|-z\rangle = |1\rangle$) and diagonal basis σ_x (i.e., $|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$). Thus the states of the B and C photons at Alice are randomly in one of the four states $\{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$ independently. She then sends the photon B to Bob and C to Charlie. Bob and Charlie choose randomly the two unitary operations $U = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ for most photons except those chosen randomly for eavesdropping check. For the sampling photons, they choose randomly one of the two measuring bases (MBs) σ_z and σ_x to measure them, and then they tell Alice their MBs and results. Alice analyzes the error rate of the sampling photons, and determines whether there is an eavesdropper in the line. This is the first eavesdropping check. For other photons, Bob and Charlie send them back to Alice after encoding with the unitary operations, and Alice measures them with the same MBs $\sigma_{_B}\sigma_{_C} \in \{\sigma_z\sigma_z,\, \sigma_z\sigma_x,\, \sigma_x\sigma_z,\, \sigma_x\sigma_x\}$ as she prepares them. The nice feature of the U operation is that it flips the state in both measuring basis, i.e., the effect of the operation U is only to negate (e.g., $|0\rangle \rightarrow |1\rangle$, $|1\rangle \rightarrow |0\rangle$) the quantum states in the same measuring basis [26, 35], i.e.,

$$U|+z\rangle \;=\; -|-z\rangle,\;\; U|-z\rangle = |+z\rangle, \tag{2}$$

$$U|+x\rangle \;=\; |-x\rangle,\;\; U|-x\rangle = -|+x\rangle. \tag{3}$$

Alice will get deterministic outcome for each photon returned in an ideal condition.

For the security of whole process for QSS, Alice needs to choose randomly a sufficiently subset of result to analyze for the eavesdropping check after the quantum communication is finished. This is the second eavesdropping check for creating the multi-party private key. The difference of the state before she sends out and receives them is just the combined effect of the unitary operations performed by Bob and Charlie. As the operations do not change the photons' MBs, the three parties do not need to announce the information about the MBs for most photons except the sampling ones. Then the unitary operations I and U can represent the bits 0 and 1 respectively, and each photon can carry one bit of secret message between two parties. The total efficiency of this

QSS approaches $\eta = 100\%$ as $b_s = 1$, $b_t = 0$, $q_t = 1$.

Because some qubits have been used in the two error analysis, the efficiency is less 1. Suppose there are δ portion of transmitted qubits are used in each error checking, then the total efficiency becomes

$$\eta = (1-\delta)^2, \tag{4}$$

and $0 < \delta \leq 1/2$. In the extreme case, $\delta = 1/2$, and the efficiency becomes 25%. When δ approaches zero, η approaches 100%, and in general $0.25 \leq \eta < 1$. Usually δ is very small and is negligible, for instance as in Ref.[29], and η approaches 1.

We now discuss the security of this QSS. It is pointed out that a QSS is secure for any eavesdropper if Alice can prevent the potential dishonest one between Bob and Charlie, say Bob* from eavesdropping the quantum communication [7]. Then the security depends on the process that Alice and Charlie* can detect the dishonest one, Bob*, if he eavesdrops the quantum channel. In fact, the process of this QSS is equal to two BID-QKD protocols [26] whose security bases on two BB84 QKD protocols [3, 30, 31, 32] with single photons. Alice can synchronously create a private K_B and K_C with Bob and Charlie respectively. In the end, Alice obtains the key $K_A = K_B \oplus K_C$. For preventing Bob* from eavesdropping, Alice and Charlie* just accomplish a BID-QKD process which is secure using single photons as quantum information carrier with two eavesdropping checks as a unknown state cannot be cloned [4], and the action of Bob* will disturb the quantum system and introduces error in the result in K_{C*}. The relation between the information $I_0(\varepsilon)$ and the error rate ε introduced by Bob* can be obtained

$$I_0(\varepsilon) \leq -\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2(1-\varepsilon). \tag{5}$$

The probability $P_d = \varepsilon$ that Bob* is detected will increase with the information $I_0(\varepsilon)$. If the error rate is low, the information $I_0(\varepsilon)$ is small, and then the parties can distill a private key with privacy amplification [2]. Otherwise, they abandon the result. Certainly, the post-processing should include the error correction part.

It is straightforwardly to generalize this QSS to multi-party secret sharing. Alice need only prepare a n-photon product state $|\psi\rangle_A$ and sends them to the other parties respectively, i.e., she sends the i-th photon to the i-th party. The total wave function Alice prepares is

$$|\psi\rangle_A = \prod_{i=1}^{n} \otimes |\phi\rangle_i, \tag{6}$$

where $|\phi\rangle_i \in \{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$. In this way, the multi-party QSS protocol is composed of n BID-QKD protocols.

Another function of QSS is to split the secret message [6, 7]. The present QSS protocol can be used to accomplish the task if we modify some part of the procedures following the ideas in quantum secure direct communication [33, 34, 35, 36, 37, 38]. We also restrict our discussion to three parties. There are two possible ways for doing the secret splitting. The first one follows the idea in the Ping-Pong deterministic secure communication protocol [33, 34] in which the photons are transmitted one by one and it is asymptotically secure when the number of the qubits transmitted is large [33]. The other one is to use the quantum secure direct communication (QSDC) protocol [35] in which the photons are transmitted in a quantum data block and the message is encoded after the parties of communication confirm that the quantum channel is secure [35, 36]. For secret splitting, Alice prepares a random number string L, and adds it to the secret message S, i.e., $G = L \oplus S$. The task of splitting the message is that Alice sends the string L to Bob and G to Charlie, and they can read out the message $S = L \oplus G$ when they collaborate. To this end, Alice requires Bob and Charlie send to her the polarized photons B and C. Assume the states of photons sent by Bob and Charlie are $|\phi\rangle_B$ and $|\phi\rangle_C$ respectively, where $|\phi\rangle_B, |\phi\rangle_C \in \{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$. Alice chooses randomly the control mode or the message mode, similar to Refs. [33] for the photons B and C independently . When she chooses the control mode, Alice measures the photons one of the two measuring bases(MBs) , σ_z and σ_x, randomly. She requires Bob or Charlie to publish her or his information about the state of the polarized photons. When the message mode is chosen, Alice encodes L and C on the states $|\phi\rangle_B$ and $|\phi\rangle_C$ with the unitary operation I or U according to the bit 0 or 1 in L and G. She uses the results obtained with control mode as the sampling photons to analyze the error rate and determines whether there is an eavesdropper in the line. Alice needs to add some redundancy randomly on the sequence of B and C photons using the unitary operations I and U.

In fact, this protocol for splitting the secret message is similar to two Ping-Pong protocols with single photons [34]. The difference is just that the states of the photons are prepared with two sets of MBs σ_z and σ_x randomly as compared to only a single MB in Ref. [34]. Though a small difference, it improves the security largely. The relation between the information obtained by an eavesdropper successfully and the probability that the parties detect her/him is the same as that for creating a private key, shown in equation (5).

Taking the probability of choosing sampling photons for eavesdropping check p_s into account, the probability for Bob* (Eve) to eavesdrop each qubit successfully is

$$P(1, p_s, \varepsilon) = \frac{1-p_s}{1-(1-\varepsilon)p_s}. \tag{7}$$

If Bob* (Eve) eavesdrops n bits of the qubits transmitted, the probability for Bob* (Eve) to successfully eavesdrop becomes

$$P(n, p_s, \varepsilon) = (\frac{1-p_s}{1-(1-\varepsilon)p_s})^n. \tag{8}$$

For $\varepsilon, p_s > 0$, the probability $P(n, p_s, \varepsilon)$ decrease exponentially. When the n is sufficiently large, it approaches zero.

The information that Bob*(Eve) successfully eavesdrops is $I(\varepsilon) = nI_0(\varepsilon)$ which is small with a low error rate. For example, if $\varepsilon = 0.1, n = 10000, P_s = 0.1$, then $I_0(\varepsilon = 0.1) \leq 0.47$, $P(10000, p_s, \varepsilon) = 10^{-48}$.

The other way for splitting the secret message can improve the security with the QSDC protocol [35] based on quantum data block [35, 36] at the cost of storing the quantum states for some times. The whole quantum communication can be divided into two procedures [35]: (1) the secure doves sending phase; (2) the message coding and doves returning phase. It equals to two quantum one time pad QSDC [35]. In the first phase, Bob and Charlie prepare their quantum state string L and G independently with the two MBs, σ_z and σ_x. It means that Bob and Charlie send a group of doves to Alice respectively. In the second phase, Alice, Bob and Charlie determine whether there is an eavesdropper or dishonest one monitoring the quantum channel. Alice encodes the message on the two groups of the doves if there is no one eavesdropping the quantum channel, and sends them back to Bob and Charlie. Otherwise, they abort the communication.

For eavesdropping check, Alice has to store the two sequence of quantum states that Bob and Charlie prepare with the two MBs randomly and send to her. The security is discussed in Ref. [35] in an ideal condition. With a noisy and lossy channel, the quantum communication can be strengthened with quantum privacy amplification [39].

In order to be secure in practice, single photon source and quantum data storage technique are required. These techniques are principally available [23, 24, 25, 40, 41]. With the improvement of technology, the technique may be practically used for quantum information.

In summary, we have proposed a QSS protocol for creating a private multi-party key following the idea in bidirectional QKD with practical faint laser pulse [26]. The QKD with high total efficiency is useful for QSS as it reduce the resource requirement for secret sharing.

This work is supported by the National Natural Science Foundation of China under Grant Nos. 10435020, 10254002, A0325401, 60433050 and 10325521, the National Fundamental Research Program under Grant No. 001CB309308, the SRFDP program of Education Ministry of China.

[1] G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, J. Amer. Inst. Elec. Eng., Vol. **45** (1926), 109-115.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] C. H. Bennett and G. Brassad, *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore*, India (IEEE, New York, 1984), PP.175-179.

[4] W. K. Wootters, and W. H. Zurek, Nature (London) **299**, 802 (1982).

[5] G. R. Blakley, in *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979), pp.313-317; A. Shamir, Commun. ACM **22**, 612 (1979).

[6] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A, **59**, 1829(1999).

[7] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[8] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999);

[9] D. Gottesman, Phys. Rev. A **61**, 042311 (2000);

[10] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).

[11] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001);

[12] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002);

[13] T. Tyc and B. C. Sanders, Phys. Rev. A **65**, 042310 (2002);

[14] S. Bagherinezhad and V. Karimipour, Phys. Rev. A **67**, 044302 (2003);

[15] A. Sen, U. Sen, and M. Żukowski, Phys. Rev. A **68**, 032309 (2003)

[16] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).

[17] F. G. Deng, G. L. Long, Y. Wang, and L. Xiao, Chin. Phys. Lett. **21**, 2097 (2004).

[18] Y. M. Li, K. S. Zhang, and K. C. Peng, Phys. Lett. A **324**, 420 (2004).

[19] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).

[20] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[21] H. K. Lo, H. F. Chau, and M. Ardehali, e-print quant-ph/0011056.

[22] W. Y. Hwang, I. G. Koh, and Y. D. Han, Phys. Lett. A **244**, 489 (1998).

[23] C. Liu, Z. Dutton, C. H. Behroozi, and L. V. Hau, Nature (London) **409**, 490 (2001).

[24] D. F. Philips, A. Fleischhauer, A. Mair, R. L. Walsworth, and M. D. Lukin, Phys. Rev. Lett. **86**, 783 (2001).

[25] C. P. Sun, Y. Li and X. F. Liu, Phys. Rev. Lett. **91**, 147903 (2003).

[26] F. G. Deng and G. L. Long, Phys. Rev. A **70**, 012311 (2004).

[27] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).

[28] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).

[29] Hoi-Kwong Lo, H. F. Chau and M. Ardehali, efficient Quantum Key Distribution Scheme And Proof of Its Unconditional Security, quant-ph/0011056.

[30] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[31] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[32] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[33] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[34] Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).

[35] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).

[36] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).

[37] Z. J. Zhang, Z. X. Man, and Y. Li, Phys. Lett. A 333, 46 (2004).

[38] F. L. Yan and X. Q. Zhang, Eur. Phys. J. B 41, 75 (2004).

[39] F. G. Deng and G. L. Long, e-print quant-ph/0408102.

[40] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999).

[41] P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang. E. Hu, and A. Imamoğlu, Science **290**, 2282 (2000).